CLAIMS

What is claimed is:

1. An apparatus comprising:

a left expansion module and a right expansion module, said left expansion module coupled to a first merged L component key XOR gate and to a third merged L component key XOR gate;

said right expansion module coupled to a key XOR gate, and to a second merged L component key XOR gate;

said key XOR gate coupled to a first selection function module (SFM), the first SFM having a first output and a second output;

said first output of the first SFM coupled to a first permutation function module (PFM) and the second output of the first SFM output is coupled to a first merged permutation and expansion function (MPE) module;

said first PFM coupled to a second collected L component XOR gate;

said first MPE module coupled to the first merged L component key XOR gate, and to the third merged L component key XOR gate;

said first merged L component key XOR gate coupled to a second SFM having a first output and a second output;

said first output of the second SFM coupled to a second PFM; and

said second PFM coupled to a first collected L component XOR gate.

2. The apparatus of claim 1 further comprising:

said second output of the second SFM coupled to a second MPE module;

said second MPE module coupled to the second merged L component key XOR gate;

said second merged L component key XOR gate coupled to a third SFM having a first output and a second output;

said first output of the third SFM coupled to a third PFM, and said second output of the third SFM coupled to a third MPE module;

said third MPE module coupled to said third merged L component key XOR gate;

said third merged L component key XOR gate coupled to a fourth SFM;

said fourth SFM coupled to a fourth PFM; and

said fourth PFM coupled to the first collected L component XOR gate.

3. The apparatus of claim 2 wherein the output of the second collected L component XOR gate is coupled to the input of the left expansion module and the output of the first collected L component XOR gate is coupled to the input of the right module function.

4. The apparatus of claim 2 wherein the key XOR gate exclusive-ors the output of the right expansion module and a first sub key block.

5. The apparatus of claim 2 wherein the first merged L component key XOR gate exclusive-ors the output of the first MPE module, the output from the left expansion module, and a second sub key block.

6. The apparatus of claim 2 wherein the second merged L component key XOR gate exclusive-ors the output of the second MPE module, the right expansion module, and a third sub key block.

7. The apparatus of claim 2 wherein the third merged L component key XOR gate exclusive-ors the output from the third MPE module, the left expansion module and a fourth sub key block.

8. A method to encrypt a block of data comprising:

splitting the block of data into a left data block and a right data block;

expanding the left data block and the right data block;

exclusive-oring, using a key XOR gate, the right expanded data block and a first sub key;

sending the output from the key XOR gate to a first selection function module (SFM), the first SFM having a first output and a second output;

sending data at the first output of the first SFM to a first permutation function module (PFM);

sending data at the second output of the first SFM to a first merged permutation and expansion function module (MPE);

exclusive-oring, using a first merged L component key XOR gate, the output from the first MPE, a second sub key and the expanded left data block;

sending the output from the first merged L component key XOR gate to a second SFM, the second SFM having a first output and a second output;

sending data at the first output of the second SFM to a second PFM;

sending data at the second output of the second SFM to a second MPE;

exclusive-oring, using a second merged L component key XOR gate, the output from the second MPE , a third sub key, and the expanded right data block;

sending the output from the second merged L component key XOR gate to a third SFM, the third SFM having a first output and a second output;

sending data from the first output of the third SFM to a third PFM;

sending data at the second output of the third SFM to a third MPE;

exclusive-oring, using a third merged L component key XOR gate, the output from the third MPE, a fourth key block, the left expanded data block, and the first MPE;

sending the output from the second merged L component key XOR gate to a fourth SFM; and

sending the output from the fourth SFM to a fourth PFM.

9. The method of claim 8 further comprising:

exclusive-oring the left data block, the first PFM output, and the third PFM output to form a left encrypted data block; and

exclusive-oring the right data block, the second PFM output, and the fourth PFM output to form a right encrypted data block.

10. The method of claim 9 wherein the left encrypted data block is obtained concurrently with sending the data to the third MPE.

11. A method comprising:

exclusive-oring, using an exclusive-or gate output from a merged permutation and expansion function module (MPE), and a sub key block; and

sending the output from the exclusive-or gate to a selection function module.

12. The method of claim 12 further comprising, sending output from the selection function module to a permutation function module.

13. The method of claim 12 further comprising sending output from the selection function module to a second MPE.

14. An apparatus comprising:

a bus;

a co-processor coupled to the bus, said co-processor having

a left expansion module and a right expansion module, said left expansion module coupled to a first merged L component key XOR gate and a third merged L component key XOR gate;

said right expansion module coupled to a key XOR gate, and a second merged L component key XOR gate;

said key XOR gate coupled to a first selection function module (SFM), the first SFM having a first output and a second output;

said first output of the first SFM coupled to a first permutation function module (PFM) and the second output of the first SFM output is coupled to a first merged permutation and expansion function (MPE) module;

said first PFM coupled to a second collected L component XOR gate;

said first MPE module coupled to the first merged L component key XOR gate, and to the third merged L component key XOR gate;

said first merged L component key XOR gate coupled to a second SFM having a first output and a second output;

said first output of the second SFM coupled to a second PFM; and

said second PFM coupled to a first collected L component XOR gate.

15. The apparatus of claim 14 further comprising:

said second output of the second SFM coupled to a second MPE module;

said second MPE module coupled to the second merged L component key XOR gate;

said second merged L component key XOR gate coupled to a third SFM having a first output and a second output;

said first output of the third SFM coupled to a third PFM, and said second output of the third SFM coupled to a third MPE module;

said third MPE module coupled to said third merged L component key XOR gate;

said third merged L component key XOR gate coupled to a fourth SFM;

said fourth SFM coupled to a fourth PFM; and

said fourth PFM coupled to the first collected L component XOR gate.

16. The apparatus of claim 15 wherein the output of the second collected L component XOR gate is coupled to the input of the left expansion module and the output of the first collected L component XOR gate is coupled to the input of the right expansion module.

17. The apparatus of claim 15 wherein the key XOR gate exclusive-ors the output of the right expansion module and a first sub key block.

18. The apparatus of claim 15 wherein the first merged L component key XOR gate exclusive-ors the output of the first MPE module, the output from the left expansion module, and a second sub key block.

19. The apparatus of claim 15 wherein the second merged L component key XOR gate exclusive-ors the output of the second MPE module, the right expansion module, and a third sub key block.

20. The apparatus of claim 15 wherein the third merged L component key XOR gate exclusive-ors the output from the third MPE module, the left expansion module and a fourth sub key block.

21. An apparatus to perform a DES iteration, said apparatus including an expansion module to receive a R input, a key XOR, a selection module, a permutation module, and a L component XOR gate, the improvement comprising:

a DES circuit to perform a series of iterations that contains no L component XOR gates, said DES circuit to include

an expansion module coupled to receive an L input;

a merged permutation expansion module, coupled to the selection module of each iteration, that results from merging the permutation module of each iteration with the expansion module of the immediately following iteration in the series;

a plurality of merged L component key XOR gates each coupled between a different one of the merged permutation expansion modules and the selection module of the immediately following iteration in the series;

a plurality of permutation modules each coupled to one selection module of a different iteration; and

a first and second collected L component XOR gates, coupled to mutually exclusive sets of the permutation modules.

22. The apparatus of claim 21 further comprising the outputs from the first and second collected L component XOR gates fed back to the expansion module coupled to the L input and the expansion module coupled to the R input respectively.

23. An apparatus comprising:

a DES circuit having an L and R component input and including,

a critical path including,

a first and second expansion modules respectively coupled to receive the L and R components;

a plurality of selection function modules coupled to each other in series by a merged permutation and expansion module coupled to a merged L component key XOR gate;

a key XOR gate coupled to the first of the selection modules in the series;

a first of a plurality of permutation modules coupled to the last of the plurality of selection function modules in the series; and

a non-critical path including,

a second L component collection XOR module, said first and second L component collection modules coupled to mutually exclusive groups of the plurality of permutation modules, wherein each of the plurality of permutation modules is coupled to a different one of the selection function modules.

24. The apparatus of claim 23 wherein the output from the first L component collection module is fed back to the L component input, and the output from the second L component collection module is fed back to the R component input.